REMARKS

This Amendment is fully responsive to the final Office Action dated December 28, 2010, issued in connection with the above-identified application. Claims 1, 3-10, 27-29 and 34 are pending in the present application. With this Amendment, claims 1, 5, 27, 29 and 34 have been amended. No new matter has been introduced by the amendments made to the claims. Favorable reconsideration is now respectfully requested.

I. Interview Summary

The Applicants thank Examiner Popham for granting the telephone interview (hereafter, "interview") that was conducted on March 2, 2010 with the Applicants representative.

Specifically, it was noted that Nakano discloses encryption keys that are designated by designating a node key which has a matching invalidation pattern to the encryption key, while sequentially referring to the nodes from the root node to the child nodes. More specifically, in Nakano, the root node is designated first, and the node keys are sequentially designated starting from the root node. Thus, the same node keys are designated as long as the combination of invalid nodes does not change.

In contrast, it was noted that, the present invention (as recited in independent claim 1) includes a terminal node (which has not been invalidated) can be selected at random when selecting one terminal node at the beginning. For this reason, it is possible to select a different key group even when the combination of the invalidated nodes does not change.

At the conclusion of the interview, the Examiner suggested that it may be helpful to further amend the claims to include the term "randomly."

II. Objection to the Specification

In the Office Action, the Examiner objects to the specification on page 10, lines 8-12 because the Applicants have not described a communication network being distinct from a recording medium, which appears to be the Applicants' intent. For example, the way the specification currently reads, the Examiner alleges that the recording medium may be interpreted as including a CD-ROM and a communication network. Accordingly, the Examiner suggests amending the specification to read "but also could be distributed via a communication network or on a recording medium such as a CD-ROM."

The Applicants have amended the specification on page 10, lines 8-12 to be consistent with the suggestions by the Examiner. That is, page 10 lines 8-12 of the specification have been amended to read "but also could be distributed via a communication network or on a recording medium such as a CD-ROM." (Emphasis added). Withdrawal of the objection to the specification is respectfully requested.

III. Claim Rejections under 35 U.S.C. 103(a)

In the Office Action, claims 1, 3-10, 29 and 34 have been rejected under 35 U.S.C. 103(a) as being unpatentable over Nakano (International Application No. WO 02/078419, hereafter "Nakano") in view of Lao (U.S. Patent No. 7,343,324, hereafter "Lao"). The Applicants have amended independent claims 1, 29 and 34 to more clearly distinguish the present invention from the cited prior art. Independent claim 1 (as amended) recites the following features:

"[a] content distribution server that encrypts a content and distributes the encrypted content to content output apparatuses connected to the content distribution server via a network, each of the content output apparatuses decrypting the encrypted content and outputting the decrypted content, the content distribution server comprising:

a key information storage unit operable to hold a node encryption key group that is a set of node encryption keys which are previously assigned to the content output apparatuses using a predetermined key assignment method;

an encryption key group selection unit operable to select, from among the node encryption key group, at least one node encryption key as a selected node encryption key group;

a content decryption key selection unit operable to generate an encrypted content decryption key group that includes at least one encrypted content decryption key obtained by encrypting a previously given content decryption key using the at least one node encryption key in the selected node encryption key group;

a content receiving unit operable to receive a content via the network;

an encryption unit operable to encrypt the content using a content encryption key which is previously given as a pair with the content decryption key; and

a transmission unit operable to distribute the encrypted content and the encrypted content decryption key group to the content output apparatuses,

wherein the key assignment method has a tree structure in which a plurality of content output apparatuses serve as nodes, and includes:

classifying the nodes into a plurality of levels from a 0^{th} level through an nth level, n being 1 or a larger natural number; and

selecting, as terminal nodes in the tree structure, nodes each of which does not have a child node, from among the nodes, and

said encryption key group selection unit selects the selected node encryption key group so that the selected node encryption key group includes at least one node encryption key that is set for a terminal node and at least one node encryption key that is set for a node other than the terminal nodes by randomly selecting a node encryption key that is set for a terminal node among the terminal nodes and then further selecting a node encryption key assigned to a content output apparatus to which the selected node encryption key is not assigned." (Emphasis added).

The features emphasized above in independent claim 1 are similarly recited in independent claims 29 and 34 (as amended). Specifically, independent claim 29 is a computer-readable recording medium and claim 34 is a method, and both claims recite steps directed at the features emphasized above in independent claim 1. Additionally, the features emphasized above in independent claim 1 (and similarly recited in independent claims 29 and 34) are fully supported by the Applicants' disclosure.

In the present invention (as recited in independent claims 1, 29 and 34), an encryption key group selection unit (or a step) selects a node encryption key group so that the node encryption key group includes at least one node encryption key that is set for a terminal node and at least one node encryption key that is set for a node other than the terminal nodes by randomly selecting a node encryption key that is set for a terminal node among the terminal nodes and further selecting a node encryption key that is assigned to content output apparatus to which the selected node encryption key is not assigned.

As a result, a terminal that is not invalidated can be selected at random. Therefore, it is possible to select a different node key group even when the combination of the invalid nodes does not change. Accordingly, a node encryption key group including node encryption keys different from a previous selection can be selected upon receipt of a new content, which produces distinct advantages such as increasing tolerance to unauthorized attacks.

In the Office Action, the Examiner relies on the combination of Nakano and Lao for disclosing or suggesting all the features recited in independent claims 1, 29 and 34. However, the Examiner relies primarily on Nakano, for disclosing or suggesting the features of the

encryption group selection unit or step of the present invention.

However, the Applicants assert that Nakano fails to disclose all the features of the encryption key group selection unit or step of the present invention. As noted above, the Applicants have amended independent claims 1, 29 and 34 to be consistent with the suggestions made during the interview with the Examiner. Accordingly, independent claims 1, 29 and 34 should be distinguishable from the cited prior art for at least similar reasons noted during the interview.

Specifically, Nakano discloses a technology in which the encryption key is to be used in encrypting the content key or designated by designating a node key which has a matching invalidation pattern to the encryption key, while sequentially referring to the nodes from the root node to the child nodes. More specifically, in Nakano, the root node is designated first. Subsequently, the node keys are sequentially designated starting from the root node. Thus, the same node keys are designated as long as the combination of invalid nodes does not change.

In contrast, in the present invention (as recited in independent claims 1, 29 and 34) a terminal node that is not invalidated can be selected at random when selecting one terminal node at the beginning of the process. For this reason, it is possible to select a different node key group even when the combination of the invalid nodes does not change. Accordingly, a node encryption key group including node encryption keys different from a previous selection can be selected, upon receipt of a new content. The present invention (as recited in independent claims 1, 29 and 34) provides a distinct advantage of increasing tolerance to unauthorized attacks.

Moreover, as noted above, Lao is not relied on by the Examiner for disclosing or suggesting the features of the encryption key group selection unit (or step) of the present invention. Regardless, after a detailed review of Lao, the reference fails to overcome the deficiencies noted above in Nakano. Accordingly, no combination of Nakano or Lao would result in, or otherwise render obvious, independent claims 1, 29 and 34 (as amended). Likewise, no combination of Nakano and Lao would result in, or otherwise render obvious, claims 3-10 at least by virtue of their dependencies of independent claim 1.

In the Office Action, claims 27 and 28 have been rejected under 35 U.S.C. 103(a) as being unpatentable over Nakano in view of Lao, and further in view Asano (U.S. Publication No. 2003/0051151, hereafter "Asano"). With regard to independent claims 27, the claim has been amended to be consistent with the amendments made to independent claim 1. Therefore,

independent claim 27 is distinguishable from Nakano in view of Lao for the same reasons noted above in independent claim 1. Additionally, Asano fails to overcome the deficiencies noted above in Nakano and Lao. Accordingly, no combination of Nakano, Lao and Asano would result in or otherwise render obvious, independent claim 27. Likewise, no combination of Nakano, Lao and Asano would result in or otherwise render obvious, claim 28 at least by virtue of its dependency on independent claim 27.

In light of the above, the Applicants respectfully submit that all the pending claims are patentable over the prior art of record. The Applicants respectfully request that the Examiner withdraw the rejections presented in the outstanding Office Action, and pass the present application to issue. The Examiner is invited to contact the undersigned attorney by telephone to resolve any remaining issues.

Respectfully submitted,

Masao NONAKA et al.

/Mark D. Pratt/
2010.03.22 14:49:06 -04'00'

By _____
Mark D. Pratt
Registration No. 45,794
Attorney for Applicants

MDP/clw
Washington, D.C. 20005-1503
Telephone (202) 721-8200
Facsimile (202) 721-8250
March 22, 2010